## CLAIMS

We claim:

1	1.	A method of operating a virtual private network (VPN)
2		based on IP Sec that integrates network address
3		translation (NAT) with IP Sec processing, comprising
4		the steps of:
5		configuring a NAT IP address pool;
6		configuring a VPN connection to utilize said NAT IP
7		address pool;
- 8		obtaining a specific IP address from said NAT IP
9		address pool, and allocating said specific IP address
10		for said VPN connection;
11		starting said VPN connection;
12		loading to an operating system kernel the security
13		associations and connection filters for said VPN
14		connection;

15	processin	ng a	ΙP	data	agram	for	said	VPN	connection;	and
16	applying	VPN	NAT	to	said	IP	datagı	cam.		

- The method of claim 1, wherein said VPN connection is
   configured for outbound processing, and said applying
   step comprises outbound source IP Nating.
- The method of claim 1, wherein said VPN connection is configured for some combination of inbound processing, and said applying step selectively comprises inbound source IP NATing or inbound destination IP NATing.
- 1 4. The method of claim 1, further for integration of NAT

  2 with IP Sec for manually-keyed IP Sec connections,

  3 comprising the further step of manually configuring

  4 connection keys.
- The method of claim 1, further for integrating NAT with IP sec for dynamically-keyed (e.g. IKE) IP Sec connections, comprising the further step of:
- 4 configuring the VPN connections to obtain their keys
  5 automatically.

- The method of claim 1, further for integrating NAT with

  IP Sec Security Associations, negotiated dynamically by

  IKE, wherein said starting step further comprises

  creating a message for IKE containing said IP address

  from said NAT pool; and further comprising the step of

  operating IKE to obtain dynamically negotiated keys.
- 7. The method of claim 6, further comprising the step of combining the dynamically obtained keys with said NAT pool IP address and wherein said loading step loads the result as security associations into said operating system kernel.
- 1 8. A method for allowing the definition and configuration 2 of NAT directly with definition and configuration of 3 IPsec-based VPN connections and VPN policy, comprising 4 the steps of:
- configuring the requirement for VPN NAT by a yes/no

  decision in a policy database for each of the three

  types of VPN NAT, said three types being VPN NAT type a

4

5

8		outbound source IP NAT, VPN NAT type c inbound source
9		IP NAT, and VPN NAT type d inbound destination IP NAT;
10		and
11		configuring a remote IP address pool or a server IP
12		address pool selectively responsive to said yes/no
13		decision for each said VPN NAT type.
1	9.	The method of claim 8, further comprising the step of
2		configuring a unique said remote IP address pool for
3		each remote address to which a VPN connection will be
4		required, whereby said remote IP address pool is keyed
5		by a remote ID.
1	10.	The method of claim 8, further comprising the step of
2		configuring said server IP address pool once for a
3		system being configured.
1	11.	A method of providing customer tracking of VPN NAT
2		activities as they occur in an operating system kernel
3		comprising the steps of:

journal records;

responsive to VPN connection configuration, generating

6		updating said journal records with new records for each
7		datagram processed through a VPN connection; and
8		enabling a customer to manage said journal records.
1	12.	A method of allowing a VPN NAT address pool to be
2		associated with a gateway, thereby allowing server
3		load- balancing, comprising the steps of:
4		configuring a server NAT IP address pool for a system
5		being configured;
6		storing specific IP addresses that are globally
7	·	routable in said server NAT IP address pool;
8		configuring a VPN connection to utilize said server NAT
9		IP address pool; and
10		managing total volume of concurrent VPN connections
11		responsive to the number of addresses in said server
12		NAT IP address pool.

6

1	13.	A method of controlling the total number of VPN
2		connections for a system based on availability of NAT
3		addresses, comprising the steps of:
4		configuring the totality of remote IP address pools
5		with a common set of IP addresses, said addresses being
6		configured as a range, as a list of single addresses,
7		or any combination of multiple ranges and single
8		addresses; and
9		limiting the successful start of concurrently active
10		VPN connections responsive to the number of said IP
11		addresses configured across the totality of said remote
12		address pools.
1	14.	A method of performing network address translation on
2		selected ICMP datagrams, comprising the steps of:
3		detecting selected types of ICMP type packets; and
4		responsive to said selected types, performing network
5		address translation functions on the entire datagram

including ICMP data.

1	15.	A method of performing network address translation on
2		selected FTP datagrams, comprising the steps of:
3		detecting the occurrence of FTP PORT or PASV FTP
4		commands; and
5		responsive to said command, performing network address
6		translation on the FTP data and the header.
1	16.	A system for operating a virtual private network (VPN)
2		based on IP Sec that integrates network address
3		translation (NAT) with IP Sec processing, comprising:
4		means for configuring a NAT IP address pool;
5		means for configuring a VPN connection to utilize said
6		NAT IP address pool;
7		means for obtaining a specific IP address from said NAT
8		IP address pool, and allocating said specific IP
9		address for said VPN connection;
10		means for starting said VPN connection;

11		means for loading to an operating system kernal the
12		security associations and connection filters for said
13		VPN connection;
14		means for processing a IP datagram for said VPN
15		connection; and
16		means for applying VPN NAT to said IP datagram.
1	17.	A system for definition and configuration of NAT
2		directly with definition and configuration of VPN
3		connections and VPN policy, comprising:
4		a policy database for configuring the requirement for
5		VPN NAT by a yes/no decision for each of the three
6		types of VPN NAT, said three types being VPN NAT type a
7		outbound source IP NAT, VPN NAT type c inbound source
8		IP NAT, and VPN NAT type d inbound destination IP NAT;
9		and
10		a remote IP address pool or a server IP address pool
11		selectively configured responsive to said yes/no
12		decision for each said VPN NAT type.

4

1	18.	A system for allowing a VPN NAT address pool to be
2		associated with a gateway, thereby allowing server
3		load- balancing, comprising:
4		a server NAT IP address pool configured for a given
5		system being configured for containing multiple address
6		configured as a range, as a list of single addresses,
7		or any combination multiple ranges and single
8		addresses;
9		said server NAT IP address pool storing specific IP
10		addresses that are globally routable;
11	·	a VPN connection configured to utilize said server NAT
12		IP address pool; and
13		a connection controller for managing total volume of
14		concurrent VPN connections responsive to the number of
15		addresses in said server NAT IP address pool.
1	19.	A program storage device readable by a machine,
2		tangibly embodying a program of instructions executable
3		by a machine to perform method steps for operating a

virtual private network (VPN) based on IP Sec that

	5	integrates network address translation (NAT) with IP
	6	Sec processing, said method steps comprising:
	7	configuring a NAT IP address pool;
	8	configuring a VPN connection to utilize said NAT IP
	9	address pool;
	10	obtaining a specific IP address from said NAT IP
<del></del>	11	address pool, and allocating said specific IP address
2 0 1	12	for said VPN connection;
<b>!</b> ≜ 	13	starting said VPN connection;
) N	14	loading to an operating system kernal the security
j i	15	associations and connection filters for said VPN
that the time that the that	16	connection;
	17	processing a IP datagram for said VPN connection; and
	18	applying VPN NAT to said IP datagram.

## 20. An article of manufacture comprising:

2	a computer useable medium having computer readable
3	program code means embodied therein for operating a
4	virtual private network (VPN) based on IP Sec that
5	integrates network address translation (NAT) with IP
6	Sec processing , the computer readable program means in
7	said article of manufacture comprising:

- 8 computer readable program code means for causing a 9 computer to effect configuring a NAT IP address pool;
- computer readable program code means for causing a computer to effect configuring a VPN connection to utilize said NAT IP address pool;
- computer readable program code means for causing a

  computer to effect obtaining a specific IP address from

  said NAT IP address pool, and allocating said specific

  IP address for said VPN connection;
- 17 computer readable program code means for causing a 18 computer to effect starting said VPN connection;

19		computer readable program code means for causing a
20		computer to effect loading to an operating system
21		kernal the security associations and connection filters
22		for said VPN connection;
23		computer readable program code means for causing a
24		computer to effect processing a IP datagram for said
25		VPN connection; and
26		computer readable program code means for causing a
27		computer to effect applying VPN NAT to said IP
28		datagram.
1	21.	Method for providing IP security in a virtual private
2		network using network address translation (NAT),
3		comprising the steps of:
4		dynamically generating NAT rules and associating them
5		with manual or dynamically generated (IKE) Security
6		Associations; thereafter
7		beginning IP security that uses the Security
Ω		Associations, and then

9	as IP Sec is performed on outbound and inbound
10	datagrams, selectively performing one or more of VPN
11	NAT type a outbound source IP NAT, VPN NAT type c
12	inbound source IP NAT, and VPN NAT type d inbound
13	destination IP NAT.

The method of claim 1, said NAT IP address pool

containing multiple addresses configured as a range, as

a list of single address, or any combination of

multiple ranges and single addresses.